Manual del uso de la Firma Electrónica en la Sede del Consejo Superior de Deportes

Manual de usuario

Versión 1.2

Histórico de versiones:

Versión	Fecha	Resumen de los cambios producidos
1.0	03/12/2014	Versión inicial del documento
1.1	27/04/2015	Incorporación de especificaciones a seguir si se utiliza Google Chrome a partir de su versión 42
1.2	22/05/2015	Especificaciones para más configuraciones de los clientes

1. Introducción **4**

2. Conceptos **5**

2.1. Certificados digitales **5**
2.1.1. ¿Qué es un certificado digital? 5
2.1.2. ¿Qué certificados digitales puedo usar? 5
2.1.3. ¿Cómo puedo obtener un certificado digital? 6
2.1.4. Cómo puedo verificar si mi certificado es válido 6

2.2. JAVA **6**
2.2.1. ¿Qué es JAVA? 6
2.2.2. ¿Dónde puedo descargar Java? 7

2.3. Applet de firma **7**

3. Requisitos del sistema y configuración **7**

3.1. Navegadores **7**
3.1.1. Configuración de Internet Explorer 8
3.1.2. Configuración de FireFox 10
3.1.3. Google Chrome 11

3.2. Sistema operativo **11**

3.3. Descarga y configuración del Java **11**
3.3.1. Versiones recomendadas 11
3.3.2. Configuración del Java 12

3.4. Certificados **12**
3.4.1. Instalación del Certificado Raíz de su Certificado Electrónico 12
3.4.2. Instalación del certificado raíz de la Sede del CSD 14

4. Sede del Consejo Superior de Deportes **16**

4.1. Acceso **16**

4.2. Firma **17**
4.2.1. Nueva solicitud 17
4.2.2. Subsanación de solicitudes 21
4.2.3. Presentación de alegaciones 21

5. Anexo I: Errores frecuentes **23**

5.1. Al iniciar la descarga del applet de firma, se genera una excepción **23**

5.2. Al acceder con Firefox: sec_error_reused_issuer_and_serial **23**

5.3. Al acceder con Firefox: ssl_error_renegotiation_not_allowed **24**

5.4. Internet Explorer: Error de Certificado: Exploración bloqueada **25**

5.5. Para usuarios de Firefox 9 o superior y Windows XP o Windows Server 2003 ..... **26**

5.6. Para usuarios de Explorer 8 y Windows XP **26**

5.7. Uso del java en Chrome versión 42 y posteriores **26**

1. INTRODUCCIÓN

La Sede del Consejo Superior de Deportes requiere del uso del certificado digital y de los mecanismos de firma electrónica para realizar la presentación telemática de los trámites publicados.

El uso de este tipo de tecnología depende directamente de la configuración de los equipos desde donde se utilizan, es por ello que este documento pretende por una parte centralizar las posibles configuraciones de dichos equipos en función de cada entorno y por otra recoger los errores más comunes que se producen.

Es importante recalcar que al depender directamente de cada equipo cada nueva actualización que se puede producir en cualquiera de los elementos implicados en el proceso puede requerir modificar las configuraciones propuestas. Es por ello que este documento evolucionará en función de estas nuevas actualizaciones y de los posibles errores que vayan surgiendo en el tiempo

.

2. CONCEPTOS

2.1. CERTIFICADOS DIGITALES

2.1.1. ¿Qué es un certificado digital?

Un certificado digital es una información que reside bien en una tarjeta física (por ejemplo el certificado asociado al DNI electrónico) o bien directamente en el navegador de su equipo, y que le permite identificarse y realizar ciertas gestiones a través de su ordenador, sustituyendo la firma manuscrita por la firma digital.

Permite además cifrar las comunicaciones entre su equipo y los diferentes sistemas a los que acceda, lo que garantiza

2.1.2. ¿Qué certificados digitales puedo usar?

Las aplicaciones del CSD utilizan todos los certificados admitidos por la plataforma de firma @firma. A día de hoy los certificados admitidos son los siguientes:

Entidad Certificadora	Tipos de certificados
Dirección General de la Policía	▪ DNIEOO1 ▪ DNIEOO2 ▪ DNIEOO3
Fábrica Nacional de Moneda y Timbre.	▪ FNMT CLASE 2
Autoridad de Certificación de la Comunidad Valenciana (ACCV)	▪ EC-SAFP Secretaria d'Administracio i Funcio Publica ▪ EC-AL Administracions Locals de Catalunya ▪ EC-IDCat Entitat publica de certificacio de ciutadans ▪ EC-UR Universitats i Recerca
Ziurtapen eta serbitzu enpresa, IZENPE S.A.	
Agencia Notarial de Certificación S.L. Unipersonal (ANCERT)	▪ Agencia Notarial de Certificación S.L. Unipersonal (Certificados Notariales Corporativos y Personales) ▪ Agencia Notarial de Certificación S.L. Unipersonal (Certificados para empleados) ▪ Agencia Notarial de Certificación S.L. Unipersonal (Certificados FERN) ▪ Agencia Notarial de Certificación S.L. Unipersonal (ANCERT Certificados para Corporaciones de Derecho

	Público)
ANF Autoridad de Certificación	
Banco Español de Crédito, S.A. (BANESTO)	
Camerfirma	▪ AC Camerfirma (RACER) ▪ Consejo Superior de Cámaras ▪ AC Camerfirma Certificados Camerales
Consejo General de la Abogacía (ACA)	
Firmaprofesional, S.A.	
Servicio de Certificación del Colegio de Registradores (SCR)	

2.1.3. ¿Cómo puedo obtener un certificado digital?

Lo más habitual es utilizar el certificado correspondiente al DNI electrónico o el expedido por la Fábrica Nacional de Moneda y Timbre. Puede encontrar toda la información necesaria para su solicitud, instalación y uso en las siguientes direcciones:

- DNI electrónico: http://www.dnielectronico.es/
- Certificado de persona física de la FNMT: https://www.sede.fnmt.gob.es/certificados/persona-fisica

2.1.4. Cómo puedo verificar si mi certificado es válido

La plataforma de firma @firma ofrece una página web a través de la cual verificar sus servicios, entre los que se encuentra la validación del certificado digital

https://valide.redsara.es/valide/

2.2. JAVA

2.2.1. ¿Qué es JAVA?

Es un conjunto de utilidades necesarias para poder ejecutar el *Applet* de firma que se descargará en el equipo del usuario.

2.2.2. ¿Dónde puedo descargar Java?

Habitualmente al acceder a una página en la que se requiere la descarga de un *Applet* se produce una verificación automática de si el equipo tiene instalado el java o no y en caso afirmativo de si tiene instalada la última versión.
Pero esto depende tanto del *Applet* al que se está intentando acceder, como de la configuración del equipo al que accede.

Por otra parte, cada nueva versión de java en muchas ocasiones lleva consigo cambios que obligan a los usuarios a realizar cambios en la configuración de sus equipos, incluso si ya estaban funcionando correctamente con la versión anterior.

Si no se inicia de forma automática, la descarga del java se puede realizar desde:

https://www.java.com/es/download/

En esta web puede además verificar si ya dispone de alguna versión instalada del java y verificar cual es.

2.3. APPLET DE FIRMA

Un *Applet* es una aplicación desarrollada en java que se instala en el navegador del equipo del usuario. En el caso del *Applet* de Firma, es imprescindible que se descargue y ejecute de esta manera, ya que utilizará las claves privadas del certificado y estas sólo son accesibles en el equipo y en concreto desde el navegador en el que está instalado dicho certificado.
En el caso de las aplicaciones del CSD, utilizan el *Applet* de Firma desarrollado por @firma (Plataforma de validación y firma electrónica del Ministerio de Hacienda y Administraciones Públicas de España) que funciona integrado en una página Web mediante JavaScript

3. REQUISITOS DEL SISTEMA Y CONFIGURACIÓN

A continuación se detallan los requisitos recomendados para poder hacer uso de los mecanismos de firma utilizados en las aplicaciones del CSD.

3.1. NAVEGADORES

Se recomienda utilizar alguno de los navegadores siguientes:

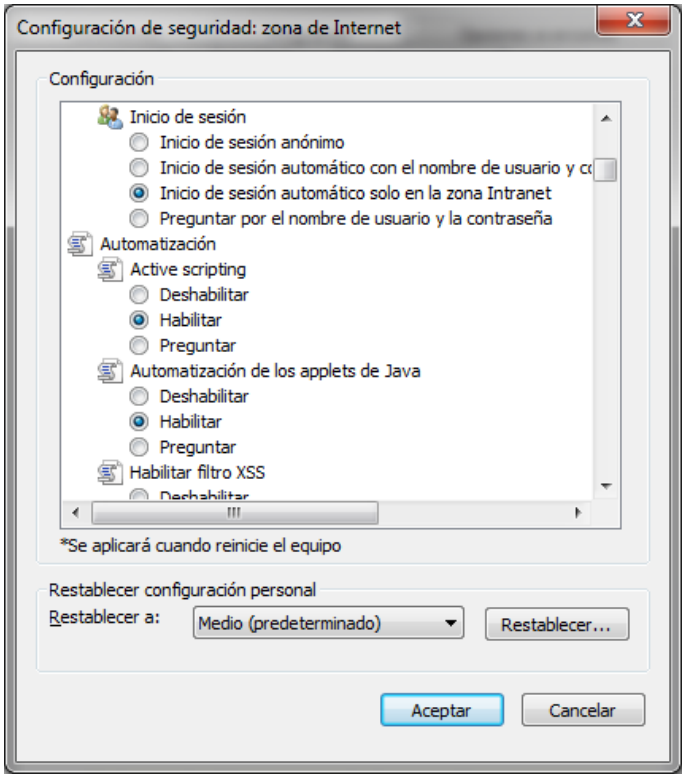
- Internet Explorer en versión 7.0 o superior
- Google Chrome
- Mozilla Firefox en versión 10.0 o superiores

3.1.1. Configuración de Internet Explorer

En caso de usar Windows 8, es necesario que ejecute el Internet Explorer desde el escritorio, porque la versión metro tiene los complementos deshabilitados y no permite la descarga del *Applet* de firma.

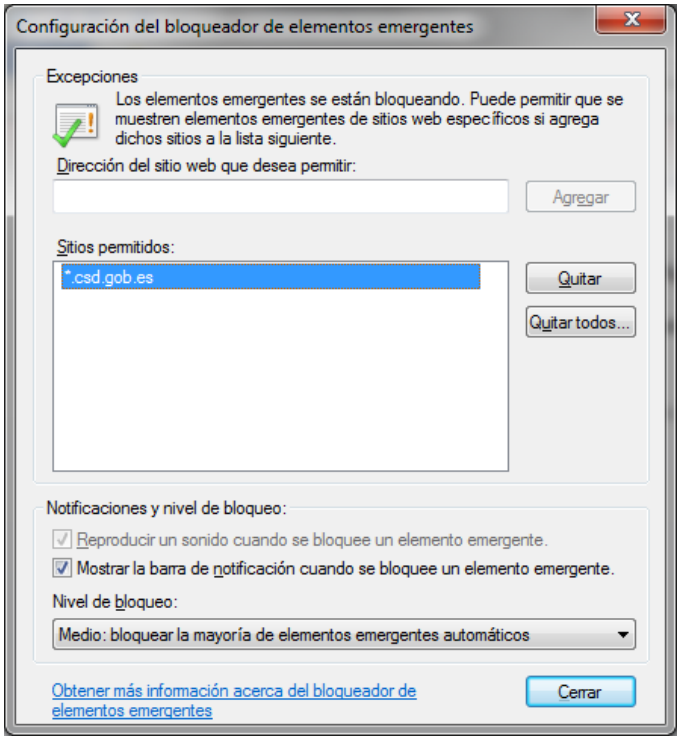
3.1.1.1. Habilitar JavaScript

Herramientas > Opciones de Internet > Seguridad > Internet > Nivel personalizado >Automatización > Active scripting > Habilitar



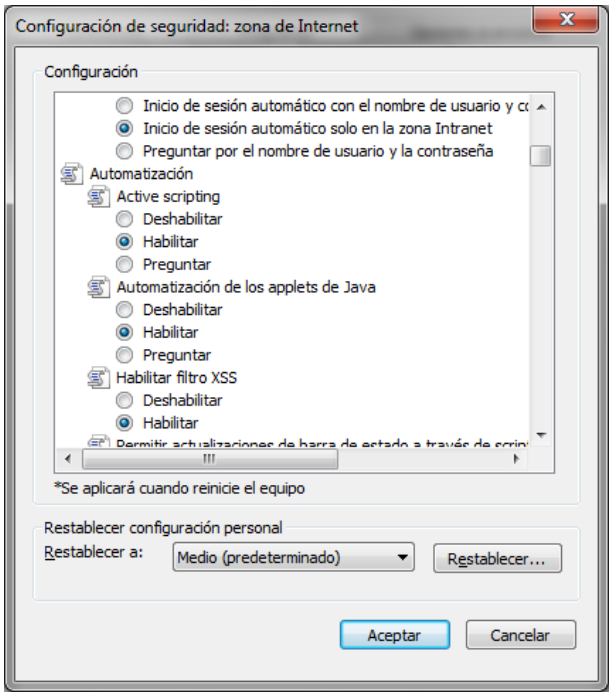
3.1.1.2. Ventanas emergentes (popups)

Desactivar el bloqueo de ventanas emergentes (Popups) para las aplicaciones del CSD. Herramientas > Bloqueador de elementos emergentes


Configuración del bloqueador de elementos emergentes
Excepciones
Los elementos emergentes se están bloqueando. Puede permitir que se muestren elementos emergentes de sitios web específicos si agrega dichos sitios a la lista siguiente.
Dirección del sitio web que desea permitir:
Agregar
Sitios permitidos:
*.csd.gob.es
Quitar
Quitar todos...
Notificaciones y nivel de bloqueo:
Reproducir un sonido cuando se bloquee un elemento emergente.
Mostrar la barra de notificación cuando se bloquee un elemento emergente.
Nivel de bloqueo:
Medio: bloquear la mayoría de elementos emergentes automáticos
Obtener más información acerca del bloqueador de elementos emergentes
Cerrar

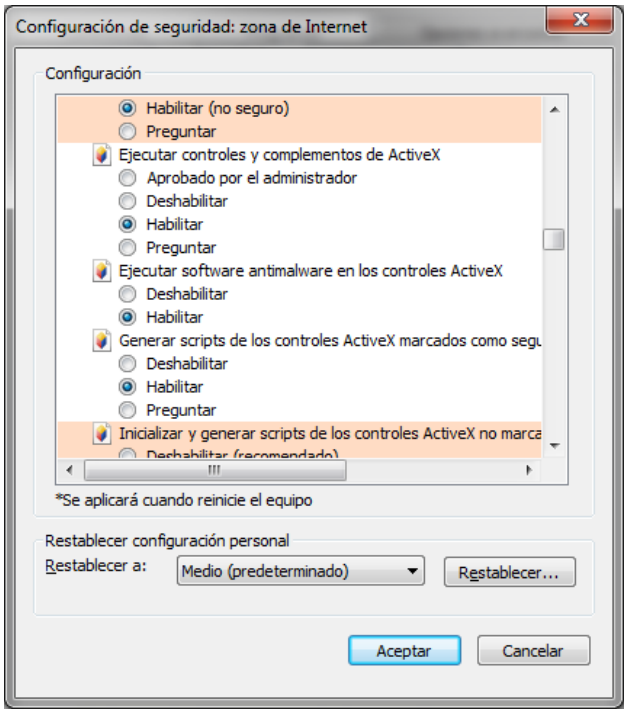
3.1.1.3. Habilitar applets de java

Herramientas > Opciones de Internet > Seguridad > Internet > Nivel personalizado >
Automatización > Automatización de los *Applets* de Java > Activar



3.1.1.4. Permitir ejecutar controles ActiveX

Herramientas > Opciones de Internet > Seguridad > Internet > Nivel personalizado > Controles y complementos de ActiveX: Ejecutar controles y complementos de ActiveX > Activar



3.1.2. Configuración de FireFox

3.1.2.1. Habilitar JavaScript

Herramientas > Opciones > Características Web o Contenido > Habilitar o Activar JavaScript

3.1.2.2. Ventanas emergentes (popups)

Herramientas > Opciones > Contenido > Bloqueador de ventanas emergentes

3.1.2.3. Habilitar applets de java

Herramientas > Complementos > Plugins > Java TM Platform > Activar

3.1.3. Google Chrome

La última versión de Google Chrome (Chrome 42) desactiva por defecto la ejecución de Java, lo que afecta a muchos sistemas que utilizan applets de Java para su funcionamiento, como el cliente de @firma.

Esto hace que los usuarios de esta última versión no puedan realizar las firmas, pero por configuración se puede activar el funcionamiento forzando al navegador. Para forzar en este navegador la activación de Java, opción que estará únicamente disponible hasta septiembre de 2015, se deben seguir estos pasos:

1. Abrir una ventana del navegador Google Chrome y escribir la dirección: chrome://flags/#enable-npapi
2. Hacer clic en el enlace "Habilitar" de la opción "Habilitar NPAPI"
3. Pulsar en el botón "Reiniciar ahora"

3.2. SISTEMA OPERATIVO

Windows en sus versiones:

- XP
- Windows 7
- Windows 8:

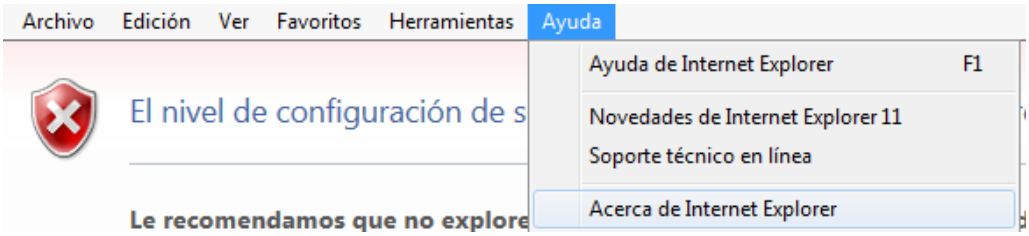
3.3. DESCARGA Y CONFIGURACIÓN DEL JAVA

3.3.1. Versiones recomendadas

Se recomienda tener instalada una versión del Java superior a la 1.7.0_51, en cualquier caso la url recomendada para la descarga del java, siempre ofrece la última versión disponible.

http://java.com/es/download/index.jsp

La versión que se descarga por defecto es la adecuada a los exploradores de 32 bits. No obstante en el caso de Internet Explorer puede verificarlo en Ayuda > Acerca de:

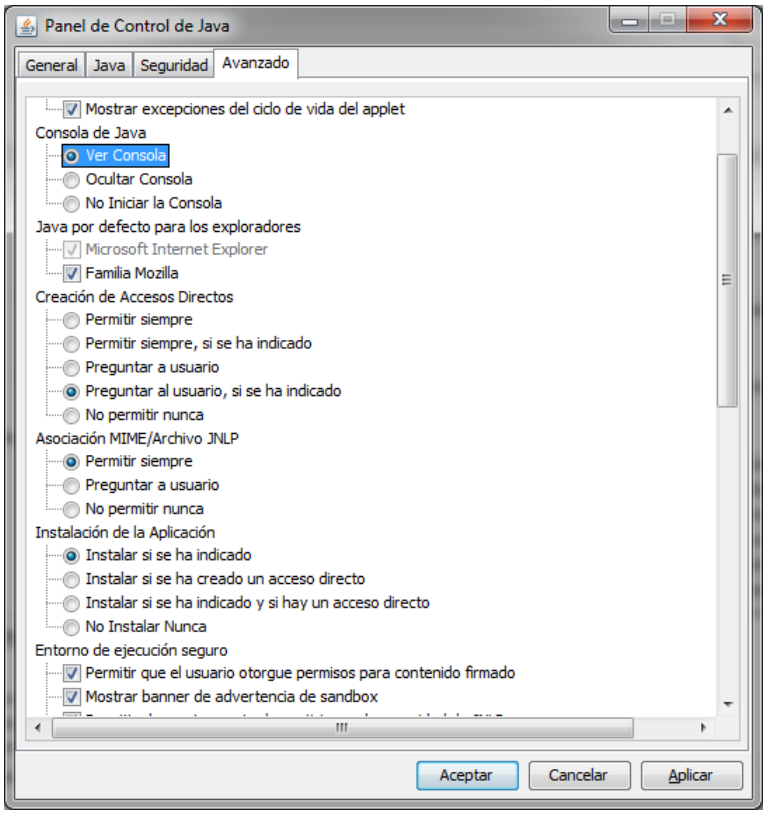


En la siguiente página puede realizar la descargar de ambas versiones:

http://java.com/es/download/manual.jsp

3.3.2. Configuración del Java

En todos los casos vamos a recomendar, aunque no es requisito, activar la consola de java, porque esto nos va a permitir verificar si en el momento de la carga del *Applet* de firma, se genera algún error que nos impida después firmar.
Para ello: Panel de control > Java > Avanzado > Consola de java, activar la opción de Ver consola

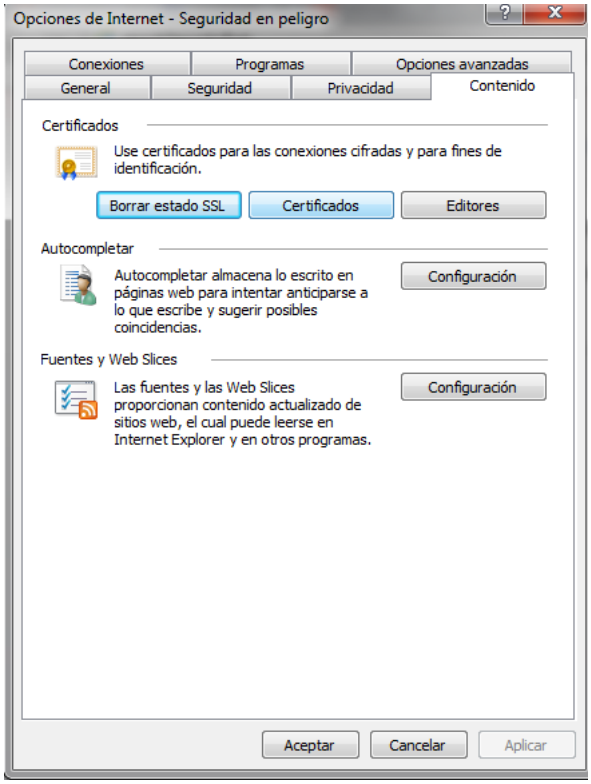


3.4. CERTIFICADOS

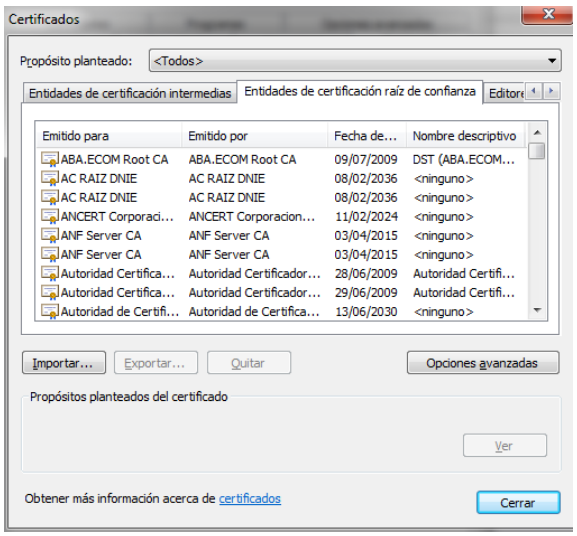
3.4.1. Instalación del Certificado Raíz de su Certificado Electrónico

Para que su certificado funcione correctamente es necesario que también tenga instalado el certificado raíz de la entidad emisora de su firma. Y que verifique si tiene habilitados “Todos los Propósitos”. Lo habitual es que ya lo tenga instalado y que esté correctamente configurado, pero es conveniente verificarlo.

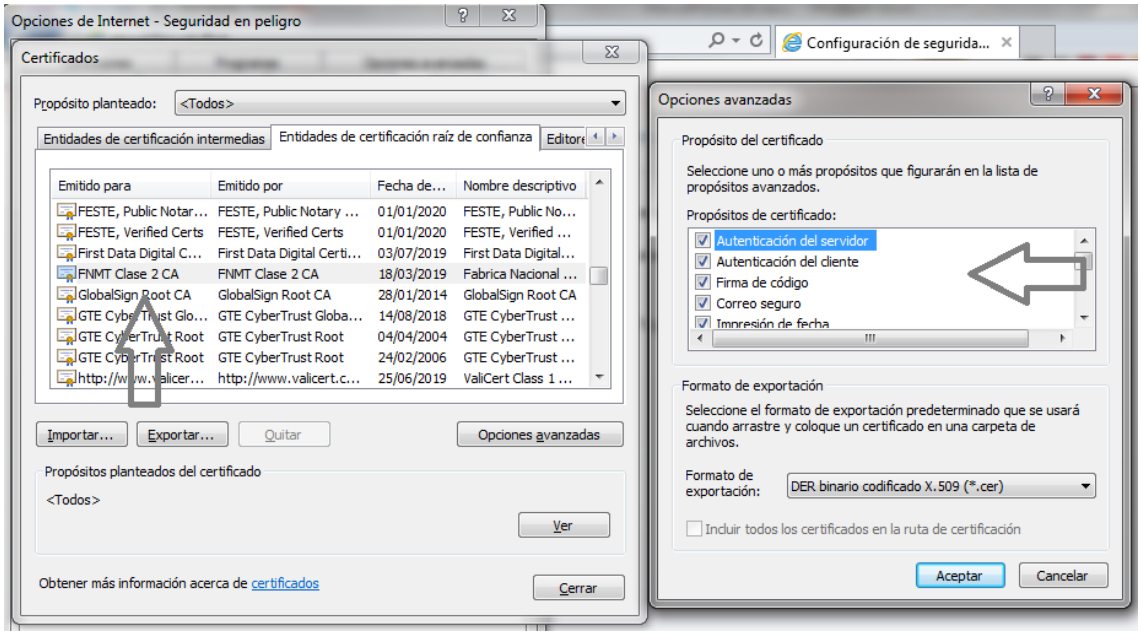
Para ello, lo más sencillo es que acceda a través del Internet Explorer, Herramientas > Opciones de Internet > Pestaña Contenido > Certificados



Accedemos y seleccionamos Entidades de Certificación Raíz Emisoras de Confianza



Buscamos el certificado raíz correspondiente a nuestro certificado digital. Una vez seleccionado el certificado, hacemos doble-click sobre él y en la pestaña Detalles > Modificar Propiedades marcar todas las opciones disponibles.



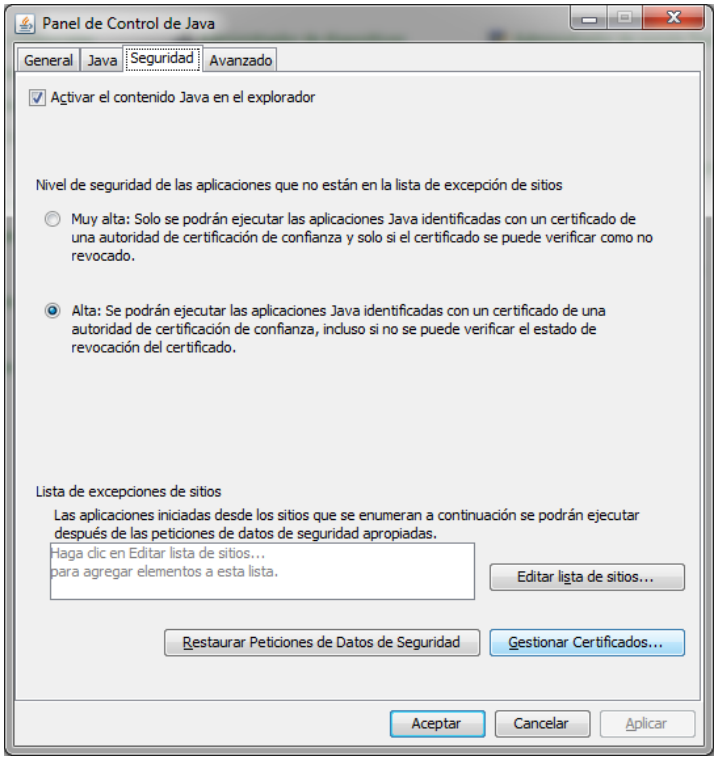
3.4.2. Instalación de los certificados raíz de la Sede del CSD

Las últimas versiones de java han subido las opciones de seguridad y esto hace que en determinados casos, impidan la descarga y ejecución de ciertos *Applets* que residen en zonas de confianza.
Esta situación se está generando por ejemplo en algunas de las Sedes Electrónicas de Organismos Públicos. En estos casos los certificados de Sede usados para garantizar la identidad de dichos portales y que garantizan seguras las comunicaciones entre el ciudadano y la Administración, no es reconocido como seguro por el Java instalado.
Esto se soluciona agregando el certificado raíz que corresponda en cada caso e indicando al Java que seguro.

En el caso de la Sede del CSD dicho certificado se puede descargar a través de esta dirección:

Parte pública del Certificado de Sede del CSD

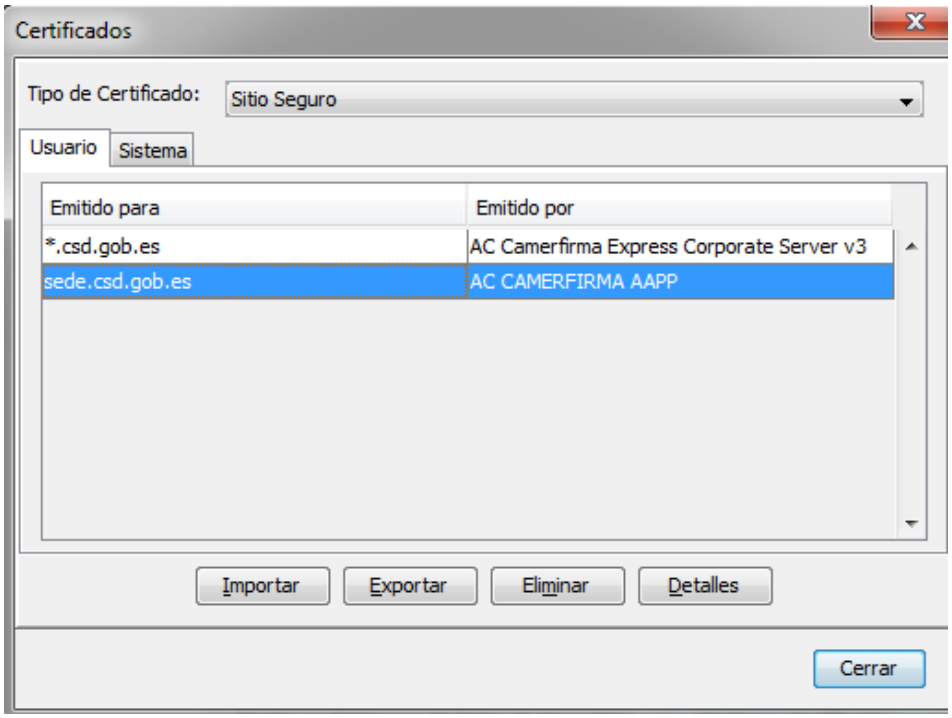
Una vez descargado en Panel de control > Java > Seguridad, seleccionar la opción de **Gestionar Certificados**:


Panel de Control de Java
General
Java
Seguridad
Avanzado
Activar el contenido Java en el explorador
Nivel de seguridad de las aplicaciones que no están en la lista de excepción de sitios
Muy alta: Solo se podrán ejecutar las aplicaciones Java identificadas con un certificado de una autoridad de certificación de confianza y solo si el certificado se puede verificar como no revocado.
Alta: Se podrán ejecutar las aplicaciones Java identificadas con un certificado de una autoridad de certificación de confianza, incluso si no se puede verificar el estado de revocación del certificado.
Lista de excepciones de sitios
Las aplicaciones iniciadas desde los sitios que se enumeran a continuación se podrán ejecutar después de las peticiones de datos de seguridad apropiadas.
Haga clic en Editar lista de sitios...
para agregar elementos a esta lista.
Editar lista de sitios...
Restaurar Peticiones de Datos de Seguridad
Gestionar Certificados...
Aceptar
Cancelar
Aplicar

Seleccione:

- Tipo de certificado: Sitio seguro
- Pestaña: Usuario

E importe el certificado descargado



En la misma pestaña anterior, seleccionar **Editar lista de sitios** y agregar **https://sede.csd.gob.es/**

4. SEDE DEL CONSEJO SUPERIOR DE DEPORTES

A continuación se exponen algunas consideraciones generales del uso de la firma en el contexto de las aplicaciones del CSD y en el acceso de la Sede del CSD.

4.1. ACCESO

Si no dispone de usuario, en el caso de la Sede, debe de solicitar su acceso a través de las opciones disponibles en función de sus necesidades:

- **Como persona física**, para realizar trámites a título personal. Requiere del uso del certificado digital.
- **Como Persona jurídica**, para realizar trámites en nombre de una entidad. Esta opción está destinada para aquellas entidades que aún no están habilitadas en la Sede y requiere que la persona que se va a registrar como Representante Jurídico lo acredite con algún documento que adjuntará a la petición de registro
- **Como habilitado para la gestión de determinados trámites**, esta opción está destinada para habilitar a un usuario a gestionar determinados trámites en nombre de una entidad que ya está registrada en la Sede

.

MIS TRAMITES
Acceso a la Oficina Virtual
Acceso
con usuario y contraseña
N.I.F / N.I.E
Contraseña
VALIDARSE
RECORDAR CONTRASEÑA
Acceso
con certificado
VALIDARSE
Se ha incorporado un nuevo mecanismo de habilitación de usuarios para realizar trámites en nombre de entidades ya registrad
propio usuario debe de solicitar dicha habilitación usando para ello su certificado digital y accediendo a través de la opción dis
Para acceder a la Oficina Virtual debe estar registrado en la misma. Si aún no lo está, puede solicitar dicho registro desde aqu
Seleccione el tipo de registro que desea realizar
Registro de persona física (Se requiere acceso con certificado)
Registro de persona jurídica
Habilitación de un usuario para uno o varios trámites en entidad ya registrada (Requiere certificado)
SOLICITUD DE REGISTRO

Una vez registrado o validada su solicitud de registro, el acceso al sistema se puede realizar de dos formas:

- Con NIF/NIE y contraseña, si no dispone de clave o la ha olvidado, puede solicitar su reenvío a través de la opción Recordar Contraseña
- Con Certificado Digital, esta es la opción obligada si lo que va es a realizar el envío y la firma de alguna solicitud, subsanación o alegación a alguna resolución provisional emitida en relación a alguno de los expedientes gestionados a través de esta sede.

4.2. FIRMA

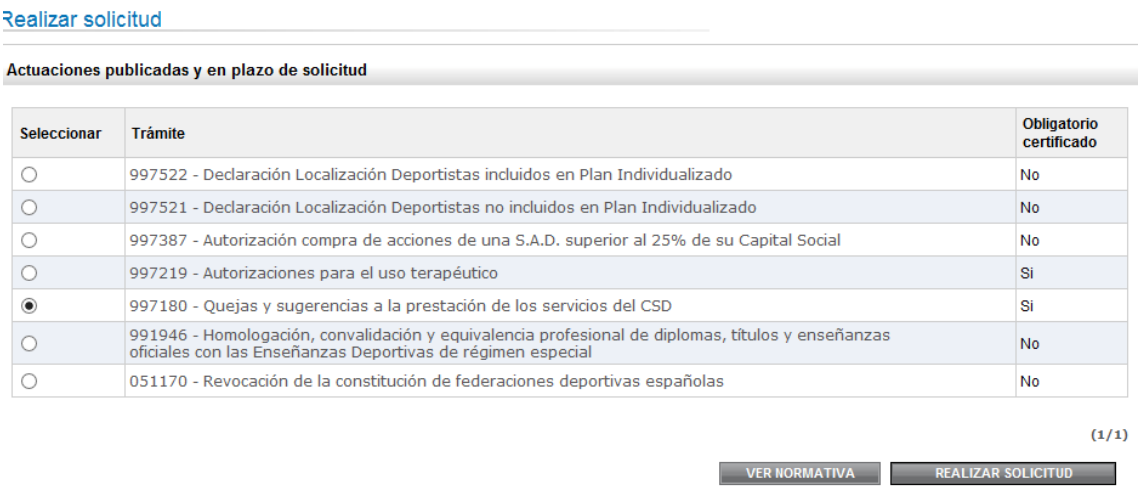
Se han incorporado mecanismos de firma en el envío de:

4.2.1. Nueva solicitud

.

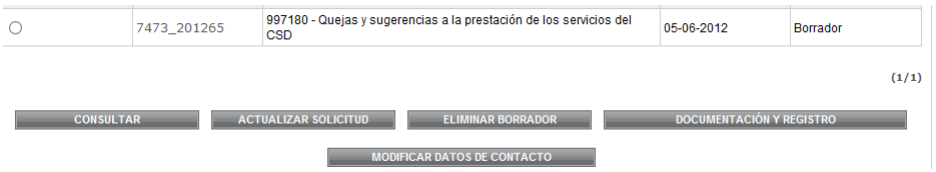
1. El acceso a la creación de una nueva solicitud se realiza a través de la opción de menú

2. Se selecciona el trámite y se pulsa el botón de Nueva solicitud

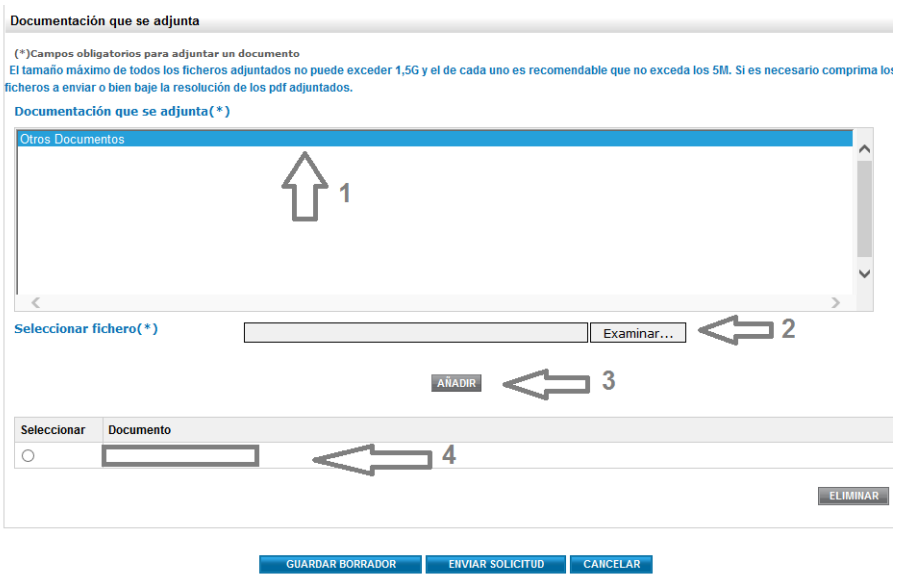

Realizar solicitud
Actuaciones publicadas y en plazo de solicitud
Seleccionar
Trámite
Obligatorio certificado
997522 - Declaración Localización Deportistas incluidos en Plan Individualizado
No
997521 - Declaración Localización Deportistas no incluidos en Plan Individualizado
No
997387 - Autorización compra de acciones de una S.A.D. superior al 25% de su Capital Social
No
997219 - Autorizaciones para el uso terapéutico
Si
997180 - Quejas y sugerencias a la prestación de los servicios del CSD
Si
991946 - Homologación, convalidación y equivalencia profesional de diplomas, títulos y enseñanzas oficiales con las Enseñanzas Deportivas de régimen especial
No
051170 - Revocación de la constitución de federaciones deportivas españolas
No
(1/1)
VER NORMATIVA
REALIZAR SOLICITUD

3. También puede proceder a firmar una solicitud que previamente haya guardado en Borrador, en este caso accederá desde la opción Seguimiento de solicitudes

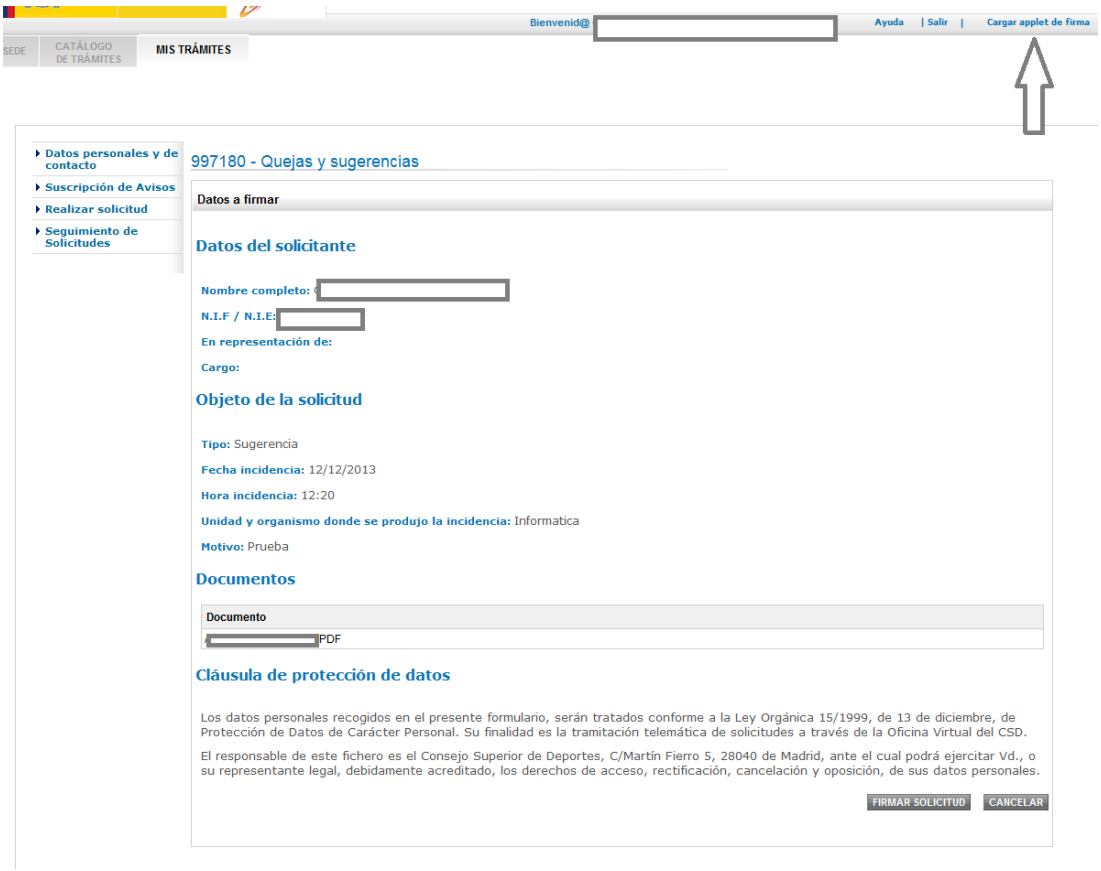
Seleccionará la solicitud a enviar y pulsará el botón Actualizar solicitud



4. En cualquiera de los dos casos, se accede al formulario correspondiente al trámite, se completan los datos solicitados, y se incorporan los documentos que correspondan en cada caso, recuerde que para agregar un documento debe de seleccionar el tipo de documento a agregar (1), seleccionar el documento (2), pulsar añadir (3) y lo verá agregado en la lista (4) tantas veces como documento tenga que adjuntar


Documentación que se adjunta
(*)Campos obligatorios para adjuntar un documento
El tamaño máximo de todos los ficheros adjuntados no puede exceder 1,5G y el de cada uno es recomendable que no exceda los 5M. Si es necesario comprima los ficheros a enviar o bien baje la resolución de los pdf adjuntados.
Documentación que se adjunta(*)
Otros Documentos
1
Seleccionar fichero(*)
Examinar...
2
AÑADIR
3
Seleccionar
Documento
4
ELIMINAR
GUARDAR BORRADOR
ENVIAR SOLICITUD
CANCELAR

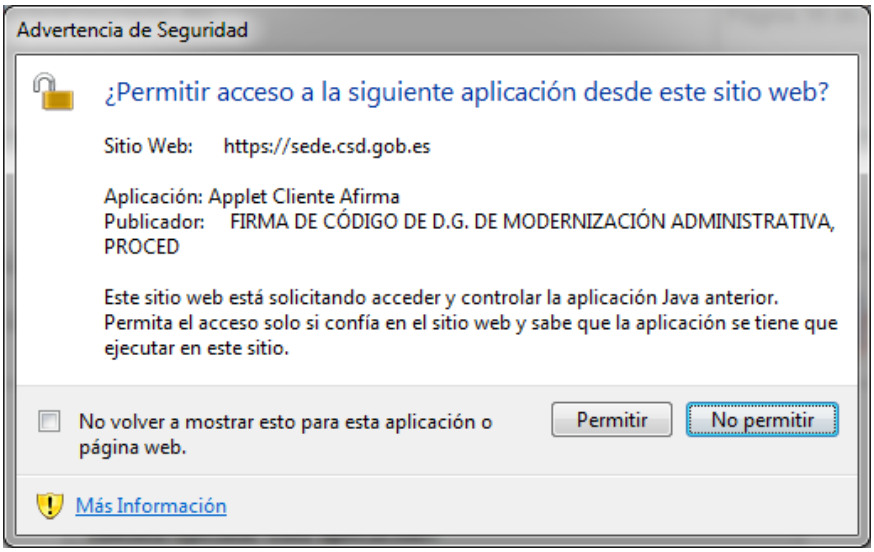
5. Una vez pulsado le botón Enviar Solicitud, se muestra la información que va a firmar, en caso de haber adjuntado documentos, verifique que sus nombres están cargados en la lista Documentos:


Bienvenid@
Ayuda | Salir | Cargar applet de firma
SEDE
CATÁLOGO DE TRÁMITES
MIS TRÁMITES
Datos personales y de contacto
Suscripción de Avisos
Realizar solicitud
Seguimiento de Solicitudes
997180 - Quejas y sugerencias
Datos a firmar
Datos del solicitante
Nombre completo:
N.I.F / N.I.E:
En representación de:
Cargo:
Objeto de la solicitud
Tipo: Sugerencia
Fecha incidencia: 12/12/2013
Hora incidencia: 12:20
Unidad y organismo donde se produjo la incidencia: Informatica
Motivo: Prueba
Documentos
Documento
PDF
Cláusula de protección de datos
Los datos personales recogidos en el presente formulario, serán tratados conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Su finalidad es la tramitación telemática de solicitudes a través de la Oficina Virtual del CSD.
El responsable de este fichero es el Consejo Superior de Deportes, C/Martín Fierro 5, 28040 de Madrid, ante el cual podrá ejercitar Vd., o su representante legal, debidamente acreditado, los derechos de acceso, rectificación, cancelación y oposición, de sus datos personales.
FIRMAR SOLICITUD
CANCELAR

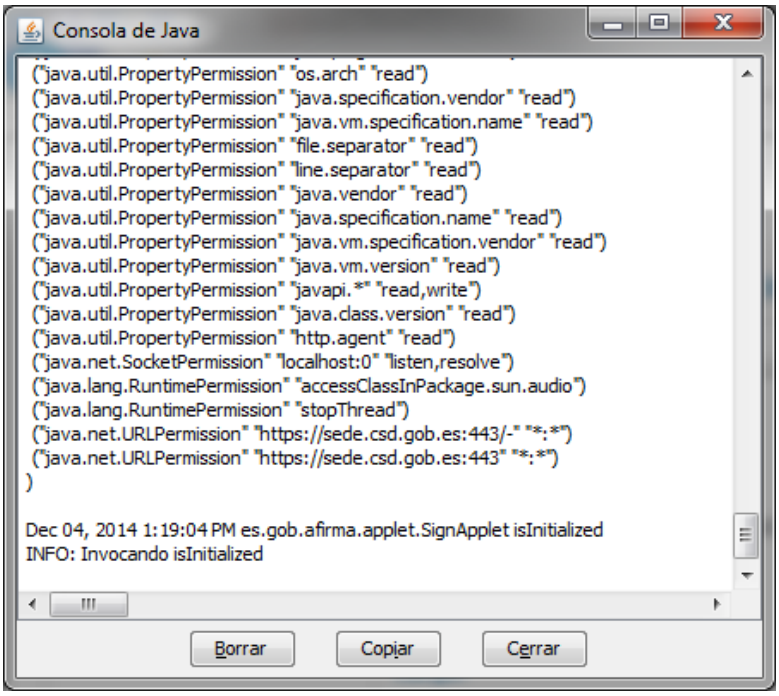
6. Al acceder a esta página, debería de cargarse de forma automática el *Applet* de firma, es conveniente tener la consola de java visible para poder verificar que se está iniciando la descarga. Si no sucede nada, puede pulsar el botón superior Cargar *Applet* de java para forzar su descarga. Si es la primera vez que accede desde su equipo, le pedirá permiso para descargar e instalar el *Applet* de firma:

¿Desea ejecutar esta aplicación?
Nombre: MiniApplet @firma
Publicador: FIRMA DE CÓDIGO DE D.G. DE MODERNIZA ...
Ubicación: https://stestiis1.csd.gob.es
Esta aplicación se ejecutará con acceso no restringido y puede poner en peligro su computadora y su información personal. Ejecute esta aplicación sólo si confía en la ubicación y el publicador que aparecen anteriormente.
No volver a mostrar esto otra vez para aplicaciones del publicador y ubicación anteriores
Más información
Ejecutar
Cancelar

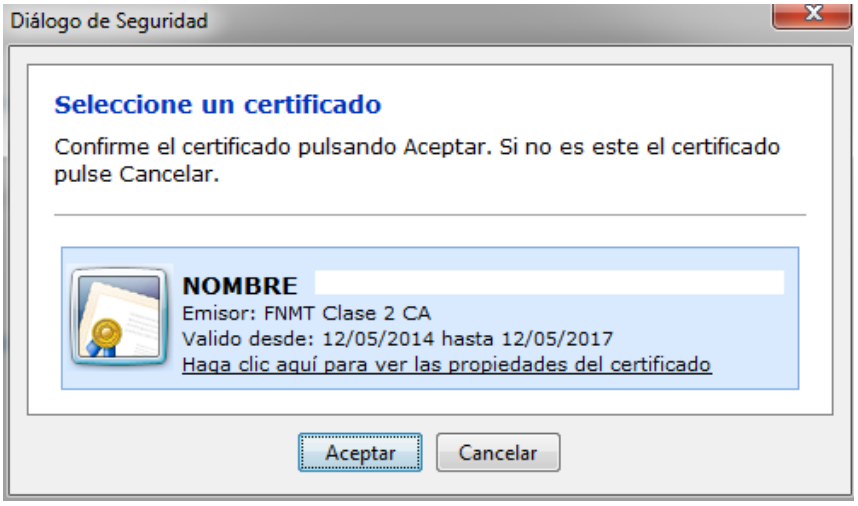
Es posible que en función de la configuración de seguridad de su equipo le solicite una nueva confirmación de acceso


Advertencia de Seguridad
¿Permitir acceso a la siguiente aplicación desde este sitio web?
Sitio Web: https://sede.csd.gob.es
Aplicación: Applet Cliente Afirma
Publicador: FIRMA DE CÓDIGO DE D.G. DE MODERNIZACIÓN ADMINISTRATIVA, PROCED
Este sitio web está solicitando acceder y controlar la aplicación Java anterior. Permita el acceso solo si confía en el sitio web y sabe que la aplicación se tiene que ejecutar en este sitio.
No volver a mostrar esto para esta aplicación o página web.
Permitir
No permitir
Más Información

Una vez finalizada la descarga, puede ver el resultado en la consola de java



Se le solicita el certificado con el que quiere realizar la firma


Diálogo de Seguridad
Seleccione un certificado
Confirme el certificado pulsando Aceptar. Si no es este el certificado pulse Cancelar.
NOMBRE
Emisor: FNMT Clase 2 CA
Valido desde: 12/05/2014 hasta 12/05/2017
Haga clic aquí para ver las propiedades del certificado
Aceptar
Cancelar

Proceda a firmar.

4.2.2. Subsanación de solicitudes

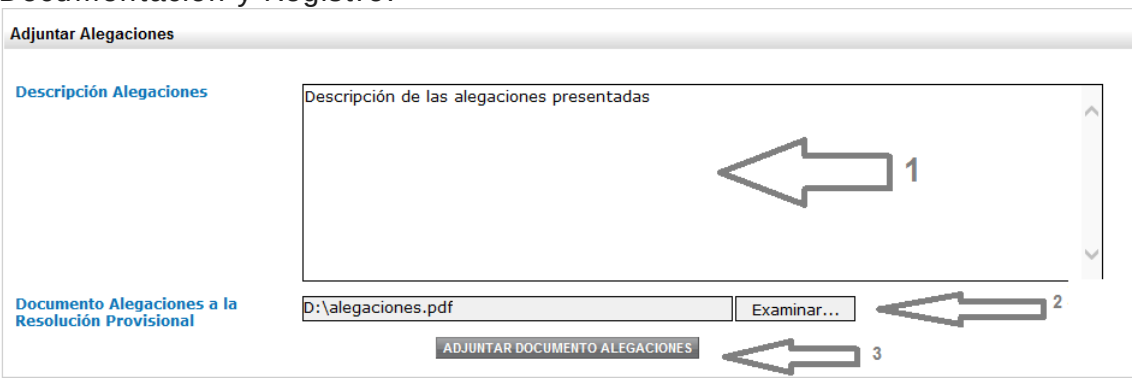
1. Sólo se pueden subsanar solicitudes que están en estado “Falta Subsanar”
2. El acceso a la subsanación de solicitudes se realiza desde la opción de Seguimiento de solicitudes

3. Seleccionar el expediente pendiente de subsanación y pulsar el botón Actualizar solicitud. Los pasos siguientes son los mismos que el punto anterior (Ver)

4.2.3. Presentación de alegaciones

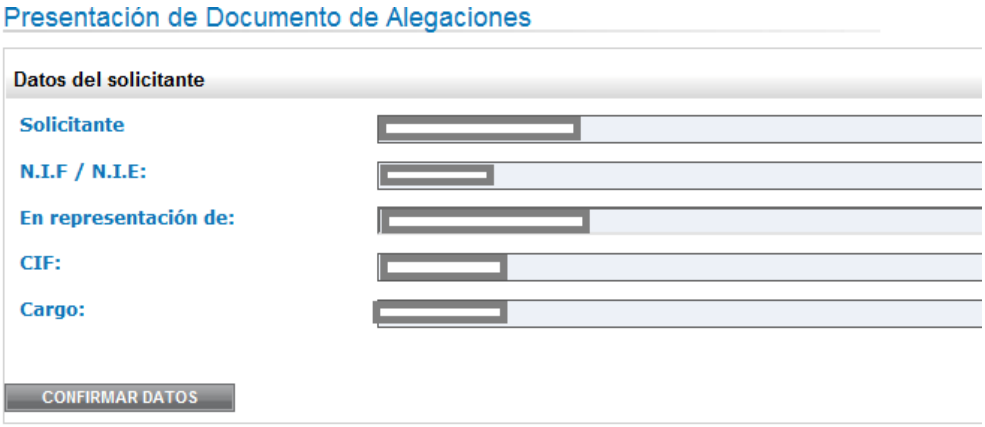
1. Sólo se pueden presentar alegaciones a solicitudes que estén en estado Resolución Provisional
2. El acceso a la subsanación de solicitudes se realiza desde la opción de Seguimiento de solicitudes

3. Seleccionar el expediente pendiente de subsanación y pulsar el botón Documentación y Registro.



Describa las alegaciones que va a presentar (1), seleccione el documento que contiene dichas alegaciones (2) y pulse el botón (3)

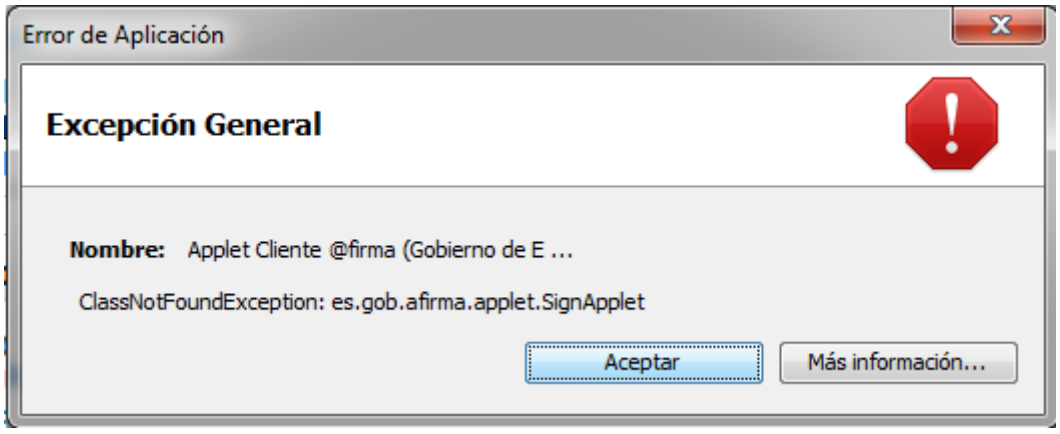
4. Se le pide confirmación de los datos



5. Y accede al formulario de firma de la misma forma que en los puntos anteriores, los pasos a dar son los mismos que los descritos en la presentación de solicitudes (ver)

5. ANEXO I: ERRORES FRECUENTES

5.1. AL INICIAR LA DESCARGA DEL APPLET DE FIRMA, SE GENERA UNA EXCEPCIÓN



Este error tiene que ver con la configuración de seguridad del java (Ver)

5.2. AL ACCEDER CON FIREFOX: SEC_ERROR_REUSED_ISSUER_AND_SERIAL

Al intentar acceder con su certificado de usuario el sistema le reporta el siguiente error:

Ha recibido un certificado no válido. Por favor, contacte con el administrador o dirección de correo electrónico de contacto del servidor y facilíteles la siguiente información:
Su certificado contiene el mismo número de serie que otro certificado emitido por la autoridad de certificación. Por favor, obtenga un nuevo certificado que contenga un número de serie único.
(Código de error: sec_error_reused_issuer_and_serial)

Cuando se produce este error, una de las soluciones que se proporcionan en los departamentos de soporte de Firefox es la siguiente:

1. Cierre Firefox
2. Busque la carpeta de perfil de Firefox que puede estar en una de estas ubicaciones:
3. En Windows 7/Vista: C:\users\[usuario]\AppData\Roaming\Mozilla\Firefox\Profiles\
4. En Windows 95/98/ME: C:\WINDOWS\Application Data\Mozilla\Firefox\Profiles\[aleatorio].[perfil]\
5. En Windows 2000/XP: C:\Documents and settings\[usuario]\Datos de programa\Mozilla\Firefox\Profiles\[aleatorio].[perfil]\
6. Y elimine al archivo cert8.dir de dicha carpeta

De todas formas, si esto le resulta complicado nuestro consejo es que pruebe a acceder a la sede con Internet Explorer.

5.3. AL ACCEDER CON FIREFOX: SSL_ERROR_RENEGOTIATION_NOT_ALLOWED

Al intentar acceder con mi certificado usando como navegador Firefox, me devuelve el error:

"ssl_error_renegotiation_not_allowed"

La página que está intentando ver no puede mostrarse porque no se ha podido verificar la autenticidad de los datos recibidos. Por favor, contacte con los administradores del sitio web para informarles de este problema.

De manera alternativa, use la opción del menú Ayuda para informar del problema de este sitio web.

Es un error independiente de este sistema, está generado directamente por el navegador, una de las soluciones que se proporcionan en los departamentos de soporte de Firefox es la siguiente:

1. Poner en el navegador Firefox about:config

2. Acceder aunque nos diga que tengamos cuidado
3. Buscar en el filtro:security.ssl.allow_unrestricted_renego_everywhere__temporarily_available
4. Poner el valor a true haciendo doble click sobre la línea
5. Cerrar y volver a acceder

5.4. INTERNET EXPLORER: ERROR DE CERTIFICADO: EXPLORACIÓN BLOQUEADA

Con las versiones de Internet Explorer a partir de la V.7, inclusive, es posible que al acceder a la Sede Electrónica del Consejo Superior de Deportes, le aparezca la pantalla que les mostramos a continuación, debido a que no está instalado el certificado raíz de la sede electrónica.

Usted, puede instalar este certificado, para ello debe pulsar sobre la opción, siguiendo los pasos que le indicamos a continuación:

1. Pulse sobre la opción: ***Vaya a este sitio web (no recomendado).***

Error de certificado: Exploración bloqueada
La configuración de seguridad actual pone a su equipo en peligro. Haga clic aquí para cambiar la configuración de seguridad...
Existe un problema con el certificado de seguridad de este sitio web.
Este sitio web presentó un certificado de seguridad emitido para una dirección de sitio web diferente.
Los problemas con los certificados de seguridad pueden indicar un intento de engañarle o de interceptar cualquier dato enviado al servidor.
Le recomendamos que cierre esta página web y no vaya a este sitio web.
Haga clic aquí para cerrar esta página web.
Vaya a este sitio web (no recomendado).

2. Sobre la barra de direcciones, pulse sobre el "Error de certificado", que aparecerá sobre un fondo en rosa, como se muestra en la figura. Aquí puede obtener información sobre el problema concreto. A continuación, pulse sobre "Ver certificados"

Error de certificado
Certificado que no es de confianza
El certificado de seguridad de este sitio web no fue emitido por una entidad de certificación de confianza.
Este problema puede indicar un intento de engaño o de interceptar datos enviados al servidor.
Se recomienda que cierre esta página web.
Acerca de errores de certificados
Ver certificados

3. En la pantalla que le sale a continuación, pulse "Instalar certificado"

5.5. PARA USUARIOS DE FIREFOX 9 O SUPERIOR Y WINDOWS XP O WINDOWS SERVER 2003

La carga del almacén de claves y certificados de Firefox 9 o superior por parte del MiniApplet @firma necesita que el sistema tenga instalado el entorno de ejecución redistribuible de Microsoft Visual C++ 2005. Si no consigue acceder a sus certificados y claves privadas desde el MiniApplet @firma, necesitará descargarlo e instalarlo manualmente:

Windows XP y Windows Server 2003 en arquitectura x86. Descarga
Windows XP y Windows Server 2003 en arquitectura x64. Descarga

5.6. PARA USUARIOS DE EXPLORER 8 Y WINDOWS XP

Para firmar la solicitud se necesita que el sistema tenga instalado la actualización de seguridad KB2809289 para poder solucionar el error "Internet Explorer no puede abrir el sitio… Operación anulada" necesitará descargarlo e instalarlo manualmente. Descarga

5.7. USO DEL JAVA EN CHROME VERSIÓN 42 Y POSTERIORES

Es necesario forzar el uso del java es estas versiones del Chrome porque por defecto viene deshabilitada.

Activación de NPAPI en Chrome versión 42 y posteriores

Si utiliza la versión 42 o posterior, es necesario realizar un paso de configuración adicional para poder seguir utilizando plugins NPAPI (Netscape Plugin Application Programming Interface).
Esta configuración es necesaria para que Chrome reconozca Java y pueda realizar el proceso de
firma:

1. En la barra de URL de Chrome, introduzca:
   chrome://flags/#enable-npapi

2. Busque ***npapi*** en la página mostrada y haga clic en el enlace Habilitar. Si la opción que aparece es Inhabilitar no es necesario que haga nada.
3. A continuación reinicie Chrome: ciérrelo y vuelva a abrirlo